This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method of securing security data stored on a computer system, comprising:

providing one of several different data keys to the computer system;

transforming the security data with the one data key in a reversible fashion to produce encoded secure data such that the one data key is required in order to perform a reverse transform and extract the security data from the encoded secure data; and,

storing the encoded secure data in a fashion such that a user authorization process is used to retrieve the encoded secure data such that the one data key and the user authorization process, in combination, provide access to the security data and such that the stored data within the computer system is encoded,

wherein a same security data is encoded with said several different data keys to provide ~~several~~ different encoded secure data for each user authorization process such that a combination of user authorization using one of said user authorization processes and any of said several different data keys allows for retrieval and decoding of the same security data.

2. (Canceled).

3. (Previously Presented) A method of securing security data stored on a computer system according to claim 1, wherein each encoded secure data is associated with one or more user authorization processes such that a combination of one or more user authorization processes and any of said several different data keys allows for retrieval and decoding.

4. (Original) A method of securing security data stored on a computer system according to claim 1, wherein the user authorization process is a biometric information verification process.

5. (Original) A method of securing security data stored on a computer system according to claim 1, wherein the data keys include a password.

6. (Currently Amended) A method of securing security data stored on a computer system, comprising:

providing a biometric information source and comparing the biometric information source against stored templates associated with the biometric information source and, in dependence upon a comparison result, pairing a biometric information source with a first individual identity;

providing one of several different data keys associated with the first individual identity, the one data key being other than stored on the computer system; and

retrieving encoded security data associated with the biometric information, and using the one data key for decoding the encoded security data,

wherein a same security data is encoded with said several different data keys to provide ~~several~~ different encoded secure data for each user authorization process such that a combination of user authorization by said biometric information source in one of said user authorization processes and any of said several different data keys allows for retrieval and decoding of the same security data.

7. (Original) A method of securing security data stored on a computer system according to claim 6, wherein the decoded security data is for performing at least one of encrypting and decrypting data on the computer system.

8. (Original) A method of securing security data stored on a computer system according to claim 6, wherein the decoded security data is for allowing access of the data to the identified individual.

9. (Previously Presented) A method of securing security data stored on a computer system according to claim 6, wherein the step of providing the biometric information source comprises imaging the biometric information source using a contact imager.

10. (Original) A method of securing security data stored on a computer system according to claim 9, wherein the contact imager is a fingerprint imager.

11. (Original) A method of securing security data stored on a computer system according to claim 6, wherein the step of providing the data key comprises the step of providing a password.

12. (Original) A method of securing security data stored on a computer system according to claim 6, wherein the step of providing the data key comprises the step of providing information stored on a smart card.

13. (Currently Amended) A method of securing data, comprising:

providing a first information sample to a computer system;

encoding one of several different data keys in dependence upon the first information sample to produce first security data, the key data for use in decoding stored encoded data;

providing at least one biometric information sample; and

securing the first security data in dependence upon at least one of the at least one biometric information sample,

wherein a same security data is encoded with said several different data keys to provide ~~several~~ different encoded secure data for each user authorization process such that a combination of user authorization using said biometric information sample in one of said user authorization processes and any of said several different data keys allows for retrieval and decoding of the same security data.

14. (Previously Presented) A method of securing data according to claim 13, wherein the step of providing a first information sample to a computer system comprises hashing the first information sample to produce a first hash value.

15. (Previously Presented) A method of securing data according to claim 13, comprising:

providing a second other information sample to the computer system;

hashing the second information sample to produce a second hash value;

encoding the key data in dependence upon the second hash value to produce second security data; and

securing the second security data in dependence upon at least one of the at least one biometric information sample.

16. (Currently Amended) A method of securing data according to claim 13, wherein the step of providing the first information sample to a computer system comprises the step of providing a password.

17. (Currently Amended) A method of securing data according to claim 13, wherein the step of providing the first information sample to a computer system comprises the step of providing information stored on a smart card.

18. (Original) A method of securing data according to claim 13, wherein the key data is used for encrypting data.

19. (Currently Amended) A method of securing data comprising:

providing a first information sample to a computer system;

providing at least one biometric information sample;

encoding the at least one biometric information sample using the first information sample;

encoding one of several different data keys in dependence upon the encoded biometric sample to produce first security data, the key data for use in decoding stored encoded data; and

securing the first security data in dependence upon at least one of the at least one biometric information sample,

wherein the first security data is encoded with said several different data keys to provide ~~several~~ different encoded secure data for each user authorization process such that a combination of user authorization using said biometric information sample in one of said user

authorization processes and any of said several different data keys allows for retrieval and decoding of the first security data.

20. (Previously Presented) A method of securing data according to claim 19, comprising:

providing a first information sample to a computer system for decoding the encoded biometric sample; and

comparing the decoded biometric sample against stored templates associated with the biometric information source.

21. (Previously Presented) A method of securing data according to claim 19 wherein the step of providing a first information sample to a computer system comprises hashing the first information sample to produce a first hash value.

22. (Currently Amended) A computer system that secures security data stored therein, comprising:

an input device that provides at least one of several different data keys to the computer system;

a processing device that encodes a same security data with said several different data keys in a reversible fashion to produce ~~several~~ different encoded secure data for each user authorization process ~~and~~ such that respective ones of the several different data keys are required in order to perform a reverse transform and extract the security data from the encoded secure data;

a memory device that stores the encoded secure data; and

a user authorization process that retrieves the encoded secure data from the memory device such that at least one of the several different data keys and the user authorization process, in combination, provide access to the security data, wherein a combination of user authorization using said user authorization process and any of said several different data keys allows for retrieval and decoding of the same security data.

23. (Previously Presented) A computer system according to claim 22, further comprising a plurality of user authorization processes, wherein each encoded secure data is associated with one or more user authorization processes such that a combination of one or more user authorization processes and any of said several different data keys allows for retrieval and decoding of the security data.

24. (Previously Presented) A computer system according to claim 22, wherein the user authorization process is a biometric information verification process.

25. (Previously Presented) A computer system according to claim 22, wherein the data keys include a password.

26. (Currently Amended) A computer system that secures security data stored therein, comprising:

means for comparing a biometric information source against stored templates associated with the biometric information source and, in dependence upon a comparison result, pairing a biometric information source with a first individual identity;

an input device that provides to the computer system ~~one of several~~ a different data key~~s~~ for each user authorization process associated with the first individual identity, the ~~one~~ data key being other than stored on the computer system; and

means for retrieving encoded security data associated with the biometric information and for using the ~~one~~ data key for decoding the encoded security data, wherein a combination of user authorization by said biometric information source in one of said user authorization processes and any of said several different data keys allows for retrieval and decoding of the same security data.

27. (Previously Presented) A computer system according to claim 26, further comprising means for performing at least one of encrypting and decrypting data on the computer system using the decoded security data.

28. (Previously Presented) A computer system according to claim 26, wherein the decoded security data allows access to the data by the identified individual.

29. (Previously Presented) A computer system according to claim 26, wherein the comparing means comprises a contact imager that images the biometric information source.

30. (Previously Presented) A computer system according to claim 29, wherein the contact imager is a fingerprint imager.

31. (Previously Presented) A computer system according to claim 26, wherein at least one of said several different data keys comprises a password.

32. (Previously Presented) A computer system according to claim 26, wherein at least one of said several different data keys is stored on a smart card.

33. (Currently Amended) A computer system that secures data stored therein, comprising:

an input device that provides a first information sample to the computer system;

means for encoding a same security data with ~~said several~~ different data keys for each user authentication process in dependence upon the first information sample to produce first security data, the key data for use in decoding stored encoded data;

a biometric input device that provides at least one biometric information sample; and

means for securing the first security data in dependence upon at least one of the at least one biometric information sample in one of said user authorization processes, wherein a combination of user authorization using said biometric information sample and any of said several different data keys allows for retrieval and decoding of the same security data.

34. (Previously Presented) A computer system according to claim 33, further comprising means for hashing the first information sample to produce a first hash value.

35. (Previously Presented) A computer system according to claim 33, wherein the first information sample comprises a password.

36. (Previously Presented) A computer system according to claim 33, wherein the first information sample is stored on a smart card.

37. (Previously Presented) A computer system according to claim 33, wherein the encoding means encrypts data using the key data.

38. (Currently Amended) A computer system that secures data stored therein, comprising:

an input device that provides a first information sample to the computer system;

a biometric input device that provides at least one biometric information sample to the computer system;

means for encoding the at least one biometric information sample using the first information sample and for encoding one of several different data keys in dependence upon the encoded biometric sample to produce first security data, the key data for use in decoding stored encoded data, wherein the first security data is encoded with said ~~several~~ different data keys for each user authorization process to provide several different encoded secure data such that a combination of user authorization using said biometric information sample in one of said user authorization processes and any of said several different data keys allows for retrieval and decoding of the first security data; and

means for securing the first security data in dependence upon at least one of the at least one biometric information sample.

39. (Previously Presented) A computer system according to claim 38, comprising:

means for decoding the encoded biometric sample using a first information sample provided by the input device; and

means for comparing the decoded biometric sample against stored templates associated with the biometric information source.